Protecting Secrets: British diplomatic cipher machines in the early Cold War, 1945-1970

8,527 words including abstract, endnotes and bibliography.

Dr David Easter

Department of War Studies

Kings College London

Strand

London WC2R 2LS

david.easter@kcl.ac.uk

Telephone: 020 7686 6168

https://orcid.org/0000-0001-6561-785

# Protecting Secrets: British diplomatic cipher machines in the early Cold War, 1945-1970

*This article examines how effectively Britain secured its diplomatic communications against hostile decryption during the early Cold War. It shows that between 1945 and 1970 the Foreign Office and the Commonwealth Relations Office introduced and operated four advanced cipher machines, Typex, Rockex, Noreen and Alvis, which produced very strong ciphers. However, Britain did suffer physical compromises of Rockex through Soviet espionage and an attack on the British embassy in Beijing. Rockex was also vulnerable to technical surveillance of its acoustic and Tempest emissions and the Soviets exploited this to read the encrypted communications of the British embassy in Moscow.*

In recent years there has been a blossoming of literature on Western signals intelligence (Sigint) in the Cold War. Ground breaking books by Richard Aldrich, Matthew Aid and Stephen Budiansky have revealed much about the activities of the main British and American Sigint agencies, Government Communications Headquarters (GCHQ) and the National Security Agency (NSA).[1] However, while the significance of Cold War Sigint is starting to be understood, comparatively little has been written about the other side of the story; the attempts by Britain and other Western states to protect their own communications from interception and decryption. In his book on GCHQ and in a separate article Aldrich has briefly discussed the British communications security agencies and two Cold War cipher machines.[2] John Ferris and Christopher Smith have also written important essays on the development of the Typex and Rockex cipher machines in the Second World War and the improvement of British signals security.[3] But so far there has been no detailed analysis of how Britain secured its diplomatic communications in the early Cold War. Yet this was a

vital task, for as Ferris observed: 'Governments have as much to gain from defending their own secret messages as attacking those of foreign states – if not more.'[4]

One way to approach this topic is to investigate the cipher machines used in the early Cold War by the two British diplomatic services, the Foreign Office and the Commonwealth Relations Office (CRO). For many years these machines were shrouded in official secrecy but fresh document releases by GCHQ, the NSA and the Foreign Office's Communications Department have put more information about them into the public domain. Drawing on these and other sources, this paper will show that between 1945 and 1970 the Foreign Office and the CRO operated a series of technologically advanced cipher machines (Rockex, Typex, Noreen and Alvis) and shared these machines with several Commonwealth states.[5] The article will then assess whether these cipher machines were able to protect British diplomatic communications against hostile decryption in the early Cold War. It will argue that while the cipher machines could apparently resist a purely cryptanalytical attack, at times Rockex was physically compromised and was vulnerable to Soviet technical surveillance and side channel attacks.

Before examining the cipher machines it would be helpful to outline the organisational structure which supported their development and use in the Cold War. These organisations had their origins in the Second World War which transformed official British attitudes towards cryptography. Before the war Britain had been slow to adopt cipher machines; the Foreign Office had relied on insecure book ciphers and the armed services only began to operate their first cipher machine, Typex, in the late 1930s.[6] But in the Second World War the Sigint bonanza at Bletchley Park powerfully demonstrated the importance of having secure ciphers. Furthermore, the British discovered late in the war that some of their own manual ciphers had been breached by Germany and Italy.[7] As a result in 1944 a Cypher Policy Board (CPB) was created to improve British cipher security.[8] It was supported by a

secretariat which became L Division of GCHQ.[9] Post-war cipher machine research and development was mainly carried out by the Services Communication Development Unit (SCDU), set up in 1946 and based at Dollis Hill in north London.[10] The SCDU was staffed by personnel from the General Post Office but was under the operational control of a CPB sub-committee.[11]

In 1954 most of L Division's communications security activities were transferred to a new stand-alone body, the London Communications Security Agency (LCSA).[12] This new agency became responsible for the production of cryptographic equipment and key material and it took over control of the SCDU.[13] The CPB was replaced by the London Communications Security Board which set policy for the LCSA.[14] A further reorganisation took place in 1965 when the LCSA was merged with the SCDU to form the Communications Electronics Security Department.[15] One constant throughout these organisational reshuffles was the input of GCHQ into cipher machine development and operation. Even when the LCSA was spun out of GCHQ the Sigint agency continued to provide it with advice, including cryptologic designs for new cipher equipment and security assessments.[16] This support was significant because GCHQ had acquired considerable expertise in breaking the ciphers of other countries and could therefore anticipate potential weakness in British cryptographic approaches, equipment and procedures. In effect, the poachers were advising the gamekeepers.

When the Cold War began in 1946-47 the Foreign Office was already bringing into service a sophisticated electro-mechanical cipher machine, Rockex, which had been developed during the Second World War.[17] Rockex relied on the same principle as a manual one-time pad. Put simply, in a one-time pad cipher system the message sender and receiver have secret, identical key pads with pages of randomly generated numbers. The sender manually enciphers the plain text message using the numbers from one page of the key pad and then sends the enciphered message with the page number. When the message is received, the

receiver deciphers it using the same page from the one-time pad. After the page has been used once it is torn out of the key pad and destroyed by both parties – hence the name one-time pad. If the pages in the one-time pad are not reused and the numbers are truly randomly generated, then the enciphered message should be unbreakable through cryptanalysis.

Rockex worked in a similar fashion but instead of one-time pads it used one-time key tapes with randomly generated punched holes.[18] A sender would type the plain text of an outward message on a teleprinter, producing a punched paper tape. This tape was then passed through a Rockex machine concurrently with a key tape. As Rockex mixed the two inputs, the teleprinter would print out at high speed an enciphered version of the message. At the receiver's end a tape was automatically prepared as the enciphered message came through. This tape was passed through the receiver's Rockex machine with the same key tape used by the sender and the teleprinter would print out a plain text version of the message. Both sender and receiver would destroy their key tapes afterwards. In this way two Rockex machines could provide the same high level of cryptographic security as a manual one-time pad system but could encrypt and decrypt messages far more quickly.

This combination of speed and security made Rockex very attractive to the Foreign Office and when the Rockex Mark II came into production in 1944 it was quickly put to work in Britain's most important and sensitive diplomatic posts.[19] Rockex was installed in the Washington embassy in October 1944 and the Moscow embassy in July-August 1945.[20] With the end of the Second World War it was deployed more widely and by 1948 the Foreign Office Communications Department had 32 Rockex cipher machines.[21] The machine did have some drawbacks, however, such as its need for a constant supply of bulky one-time tapes which had to be securely stored and disposed of after use. Consequently, despite Rockex's superior speed the Foreign Office maintained manual one-time pads as the encryption system for embassies with low volumes of communications traffic.[22]

It soon emerged that there was another, more serious problem with Rockex. The seemingly impregnable cipher machine had a technical weakness which could compromise its security. In his annual report for the year ending 31 July 1948, the secretary of the CPB explained that:

> It has recently come to light…that the Rockex Mark II produces severe electrical radiation which can be readily intercepted in the vicinity of the machine; when decyphering, this radiation is such that clear text may be read directly without cryptanalysis.[23]

What the CPB had come up against was a security issue that would bedevil many countries' cipher machines and other items of electrical equipment in the Cold War. As these devices operated they emitted electro-magnetic energy which could radiate in free space for up to a half a mile or travel even further if it was induced on nearby conductors like power lines or telephone lines.[24] If a hostile intelligence service intercepted and analysed these emissions from a cipher machine or a teleprinter it could potentially recreate the original plain text of an enciphered message, in effect by-passing the cipher. This security issue would later be known by the LCSA and NSA as Tempest.[25] The Mark I and II models of Rockex appear to have been powerful emitters of Tempest radiation; a later NSA paper described them as 'inherently insecure' and 'compromised by radiation.'[26]

This was a major blow to Britain's post-war communications security strategy for the CPB had envisaged that the Rockex Mark II would carry all the essential traffic of the Foreign Office, as well as that of the Chiefs of Staff and GCHQ and perhaps other departments.[27] The SCDU urgently sought ways to suppress Rockex's compromising emissions but this proved no easy task and in March 1950 the secretary of the CPB warned that Rockex production might have to be delayed.[28] The CPB asked the Treasury to give the SCDU more staff and a larger building because of the extra, unexpected work caused by the Tempest issue.[29] By 1953 the SCDU had developed new versions of Rockex (the Marks III and IV) which the British considered more secure.[30] But even so, Tempest radiation was a recurring problem for Rockex and to some extent limited where it could be used. For example, in 1957 the Foreign

Office recommended against installing a Rockex machine in the British embassy in Bangkok because of the 'radiation dangers'.[31]

While the Foreign Office grappled with Rockex, Britain's second diplomatic service, the Commonwealth Relations Office, made alternative cipher arrangements. The CRO handled Britain's relations with the Commonwealth and had diplomatic missions, called high commissions, in Commonwealth countries. For secure communications with its high commissions the CRO employed the Typex electro-mechanical cipher machine. Typex had been devised just before the Second World War and was based upon early commercial versions of the famous German Enigma cipher machine. Like Enigma it used the movement of rotors to substitute letters as they were typed into the machine.[32] Given that Bletchley Park had repeatedly broken Enigma ciphers in the Second World War, the CRO's reliance on Typex in the early Cold War might seem foolhardy but the British had substantially altered the device to make it more secure than its German counterpart. For one thing, Typex had more rotors than Enigma which meant there were far more potential rotor combinations.[33] In 1946 the British authorities decided to further modify Typex to increase its cryptographic strength.[34] The rotors and turnover mechanism were redesigned so that all rotors would turn as a message was encrypted and the machine was fitted with a pluggable 'crossover' at the entry and exit to the wiring maze.[35] This new version of Typex was ready for service in September 1950 and it was predicted that it would provide adequate cipher security for another ten years.[36] Moreover Typex had the advantage that it was a low emitter of Tempest radiation.[37] Consequently the CRO decided to use Typex rather than Rockex and it operated Typex throughout the 1950s.[38]

This decision to stick with Typex had an unfortunate consequence; since Britain's two diplomatic services were operating completely different cipher machine systems it was difficult for Foreign Office embassies and CRO high commissions to have direct, secure

communication with each other.[39] As more British colonies became independent and joined the Commonwealth the number of high commissions increased, aggravating the problem of inter-communication. In the early 1960s Duncan Sandys, the Commonwealth Relations Secretary, complained several times that it was not possible for him to address Foreign Office and CRO posts during his tours overseas without considerable repetition of enciphering.[40] But by this point Typex was already coming to the end of its cryptographic life and the Foreign Office was able to convince the CRO to harmonize encryption systems and take on Rockex as a partial replacement for Typex.[41] From 1964 Rockex was rolled out to selected CRO high commissions.[42]

In the mid-1960s the CRO and the Foreign Office also began to operate a miniaturised version of Rockex called Noreen.[43] Noreen used the same one-time key tapes as Rockex and the two cipher machines were interoperable. Noreen was however smaller, lighter and more portable and with this device the Foreign Office was able to mechanise encryption across its embassy network. Once Noreen was cleared for production in 1963 the Foreign Office distributed it to smaller diplomatic outposts that had previously depended on one-time pads and basic book ciphers.[44] As a result, between 1961 and 1965 Foreign Office book cipher usage fell from 25% to 3% of all cipher traffic.[45] But the Foreign Office also had to equip some embassies with Noreen because of what one official called the 'security weaknesses' of Rockex, most likely a reference to its Tempest emissions.[46] Noreen seems to have produced less compromising Tempest radiation than Rockex – reportedly a Noreen cipher machine did not radiate more than four feet.[47] In the 1960s it was therefore installed in several embassies where the threat of hostile interception and decryption was particularly high, such as in the Soviet Bloc capitals Bucharest, Budapest, Prague, Sofia and Warsaw.[48]

Noreen was not an ideal solution to this security problem though since it was considerably slower at enciphering and deciphering than Rockex and unsuitable for posts that had high

volumes of communications traffic.[49] What was needed was a device with a greater capacity than Noreen but without the technical security weaknesses of Rockex. In the 1960s the Foreign Office did have in development the intended successor to Rockex, known as Topic, but research on Topic progressed slowly and there were delays in starting production.[50] To fill the capability gap the Foreign Office decided to buy the Alvis cipher machine which was just coming into service with the British military.[51] Alvis was a new generation, electronic cipher machine that did not require cumbersome one-time key tapes.[52] Unlike Britain's earlier cipher machines, it had been developed in cooperation with the United States; according to Robert Stannard, the Director of the LCSA, the cryptologic principle behind Alvis was 'jointly UK/US' and the machines' original cryptologic and technical specifications relied in part on American ideas.[53] The Treasury agreed that the Foreign Office could purchase Alvis for posts where there were good operational security reasons for replacing Rockex before Topic became available.[54] In practice, the Foreign Office and CRO seem to have deployed Alvis more widely as a general replacement for Rockex. Alvis was installed in Paris, Bonn and Berlin in 1965, in Washington and Ottawa in 1966 and by 1970 it was present at the Moscow embassy.[55] It was planned that by 1974 77 British diplomatic posts would be using Alvis and 61 Noreen.[56] Just two posts, Muscat and Aden, would be left with Rockex.

The Foreign Office and the CRO were not the only users of Typex, Rockex, Noreen and Alvis for these cipher machines were also sold to Commonwealth countries, most notably Australia, Canada and New Zealand. These states were part of a Sigint alliance with Britain and the United States based around the 1954 United Kingdom-United States (UKUSA) agreement and the UKUSA partners closely cooperated in communications security.[57] It therefore made sense for Britain to supply Australia, Canada and New Zealand with its most secure cipher technology. The Australian Department of External Affairs (DEA) was able to

buy British Typex Mark 22 cipher machines and it installed Typex at its embassy in Washington and other diplomatic posts.[58] In the 1950s the DEA started to use Rockex and in the 1960s it acquired Noreen and Alvis.[59] Canada followed a similar pattern although it adopted Rockex earlier; by 1949 the Canadian Department of External Affairs already had 13 Rockex Mark IIs.[60] New Zealand operated Typex and probably Rockex.[61] Britain and its three Commonwealth allies shared the burden of maintaining their cipher machines around the world. For example, the CRO's Typex and Rockex machines in Ottawa, Canberra and Wellington were serviced by the host nations while the British Air Ministry looked after Australian and New Zealand machines in London.[62]

London also released Typex to new Commonwealth countries which were not part of the select UKUSA group. When British colonies achieved independence after 1945 London supplied them with cipher equipment to secure their communications and maintain compatible cipher services within the Commonwealth.[63] Typex cipher machines were sold at below cost price to newly independent India, Sri Lanka, Ghana and Malaya.[64] Yet these countries were treated differently to the UKUSA allies; while Britain in 1949 was willing to provide Australia with the Typex Mark 22, this model was not be for sale to India.[65] The Indians would continue to use the older, less secure Mark II version of Typex and would not even be informed of the Mark 22. In the mid-1960s the British government abandoned its policy of supplying cipher machines and cryptographic information to the new Commonwealth states, probably for cost reasons.[66]

Typex, Rockex and Noreen provided Britain and its Commonwealth allies with fast machine encryption and speeded up diplomatic communications, with embassies and high commissions able to handle a much greater volume of encrypted messages than before. What remains to be determined though is whether these cipher machines protected Britain's diplomatic messages from hostile decryption. The Sigint directorate of the Soviet KGB and

its predecessors in the NKVD, NKGB and MGB repeatedly targeted Foreign Office communications and it is likely that many other countries tried to solve British ciphers during the early Cold War.[67] With currently available sources it is difficult to assess how successful they were as the British government has not revealed whether any of its ciphers were broken and foreign intelligence services have not trumpeted any victories. A KGB officer, Yuri Noskeno, who defected to the United States in 1964, did report that there were 'some successes' in decrypting British communications but he could not remember any specific examples and may not have been referring to machine encrypted diplomatic traffic.[68]

It is possible though to examine the ways in which foreign intelligence services (and especially the KGB) might have attacked the ciphers and look for any obvious failings in British cryptographic security. There were three main approaches that an intelligence service could have taken at this time: it could intercept British diplomatic telegrams and seek to solve the cipher through pure cryptanalysis, applying mathematical techniques and linguistic analysis; it could try to obtain the cipher machines and cryptographic materials, such as key lists and key tapes. Or if it was sufficiently technologically advanced, it could carry out side channel attacks that used emissions from the machines, such as Tempest radiation and acoustic signatures, to reconstruct the message. These approaches could be complementary, as information from seized or stolen cryptographic material and analysis of Tempest radiation might aid the mathematicians and linguists working on the cipher.

In the first case, British officials were convinced that the Rockex and Noreen ciphers could not be solved through pure cryptanalysis because they were one-time machines. A CRO cipher official wrote in 1960 that 'Rockex is "one-time" and, therefore, 100% secure against cryptanalysis'.[69] The Typex cipher was theoretically solvable but the Germans had been unable to break Typex in World War Two and the Mark 22 version generated an even stronger cipher.[70] Consequently, the CRO thought that Typex was '99.9% secure' against

cryptanalysis.[71] Of course, human error could weaken the security of even the strongest cipher machine and on occasion cipher clerks did accidentally reuse a Rockex key tape to encipher a second telegram, which made the two messages concerned vulnerable to decryption.[72] But short of this type of operator error, the British authorities believed that their machine ciphers could withstand a purely cryptanalytic attack. Any intelligence agency seeking to break the cipher would need help from other sources. A LCSA paper in 1956 confidently stated that:

> The security of modern general purpose crypto systems is so high that cryptanalytical success against them will be extremely difficult, if not impossible. If an enemy is to succeed in breaking our cypher messages he will therefore depend for success on "pinching" some or all of the key data.[73]

'Pinching' was a term used at Bletchley Park in World War 2 to describe Allied seizures of Enigma cipher machines and cryptographic material, like codebooks, manuals and key settings, in raids on German ships and submarines.[74] It was obviously not possible to carry out such military attacks in peace time but in the early Cold War three British embassies were overrun by rioters (Baghdad in 1958, Jakarta in 1963 and Beijing in 1967) and these security breaches could have provided opportunities for the local intelligence services to 'pinch' cryptographic material and cipher machines. Furthermore, in 1964 Soviet fireman entered Britain's Moscow embassy and in 1961 Egyptian protestors invaded the Canadian embassy in Cairo, which operated Rockex. In most of these cases the embassy staff managed to stop cryptographic material and cipher machines from falling into hostile hands. The cipher machines were destroyed in Baghdad and in the Moscow embassy fire the cipher clerks prevented the Soviet 'firemen', who were presumed to be KGB personnel, from forcing their way into the code room.[75] In Cairo the protestors did not reach the embassy communications centre although the Canadians started to destroy the Rockex key tapes and documents.[76]

In Jakarta things were more difficult. Indonesian protestors ransacked and set alight the British embassy on 18 September 1963 but the staff were able to carry the cipher machines and cryptographic material to the strong room before they could be seized by the rioters. The ambassador, Sir Andrew Gilchrist, returned to the gutted embassy on 23 September and found that the Indonesians were trying to break into the strong room.[77] While Gilchrist remonstrated with the Indonesians Western diplomats slipped into the strong room, removed some of the most sensitive documents and 'did strategic damage to [the] code machines'.[78] The next day, amidst rumours that the Indonesian army cipher expert, Brigadier-General Rubiono Kertosati, was in the building, the British and Americans used trucks to transfer all the material from the still locked strong room to the safety of the American embassy.[79]

Britain's luck finally ran out in Beijing in 1967.[80] China was then in the turmoil of the Cultural Revolution and Britain had become the focus of the revolutionaries' anger because of its colonial control over Hong Kong. On 22 August 1967 thousands of Red Guards stormed the British embassy and amongst them were Chinese cipher experts who knew where the code machines were located in the mission.[81] Although the embassy staff carried out their emergency procedures they did not have enough time to destroy one Rockex cipher machine or move it to the strong room and the machine was captured by the Chinese.[82] It is not clear how serious a security breach this was. Without the key tapes it would have been impossible for the Chinese to read the Rockex's messages and one of the British diplomats in the embassy, John Weston, later recalled that although they lost the cipher machine, '[m]ost of the other stuff we didn't want the Chinese to get, we…succeeded in putting behind the strong-room doors'.[83] This suggests that the key tapes and other cryptographic material may have been secured in time.[84] Like the Indonesians the Chinese did try to break into the strong room but they were unable to penetrate its nine-inch thick steel doors.[85] Nevertheless, possession of the Rockex would have given Chinese cryptanalysts an opportunity to study

how the machine operated, understand its cryptologic principles and look for weaknesses that could be used in side channel attacks. The official instructions for the emergency destruction of Rockex warned that 'it is of the greatest importance to deny to any foreign power knowledge of how the machine works and, in particular, the precautionary measures taken to ensure that no spurious radiation is present.'[86] The concern seems to have been that an enemy like China might find ways to exploit Rockex's Tempest emissions.

Espionage was another, less dramatic way for opponents to 'pinch' cryptographic materials and gain information on cipher machines. Foreign intelligence agencies could recruit or insert agents in the British diplomatic services and their overseas missions. Soviet espionage especially had been a major problem for the Foreign Office in the past. During the 1930s the NKVD recruited two cipher clerks in the Foreign Office Communications Department, Ernest Oldham and John King, who gave them information about Foreign Office book ciphers.[87] Burdened with guilt, Oldham committed suicide in 1933 and after King was discovered and jailed in 1939, the Foreign Office cleaned house by replacing all the staff in the Communications Department.[88] But despite this the Soviets still had active agents in the Foreign Office in the early Cold War and at least two of these, Donald Maclean and Leonard Hinchcliffe, could access cipher machines and cryptographic materials.

Maclean was recruited by the Soviets while still a student at Cambridge University in 1934 and under their direction he worked in the Foreign Office from 1935 until 1951 with access to highly sensitive top secret documents.[89] He was eventually unmasked by an Anglo-American Sigint operation, code named VENONA, that analysed encrypted messages in the Second World War between Moscow and the NKVD/NKGB stations in the Soviet diplomatic missions in Washington and New York.[90] Maclean had served in Britain's Washington embassy between 1944 and 1948 and a handful of the decrypted VENONA telegrams from 1944 and 1945 reported the activities of a Soviet agent codenamed HOMER, who was

identified as Maclean. Unfortunately, Maclean was tipped off before he could be questioned by the British security services and he defected to the Soviet Union in May 1951.

The VENONA decrypts did not show HOMER passing cipher secrets to the Soviets but the Americans only managed to intercept and decipher a small fraction of the traffic between Moscow and the NKVD/NKGB in Washington and New York.[91] There may have been other NKVD/NKGB telegrams which did contain or refer to cryptographic material supplied by Maclean while he worked at the embassy in Washington. British and American officials believed that Maclean had given the Soviets cipher information; the former MI5 officer Peter Wright claimed in his memoirs that Maclean had 'betrayed every code he had access to in the Foreign Office.'[92] A damage assessment for the American Joint Chiefs of Staff in 1955 concluded that because of the espionage of Maclean and his accomplice Guy Burgess, 'all U.K. and possibly some U.S. diplomatic codes and ciphers in existence prior to 25 May 1951 are in possession of the Soviets and of no further use.'[93]

The Joint Chiefs' assessment is puzzling and perhaps overly alarmist for if fresh manual one-time pads and Rockex key tapes were issued, these forms of encryption should have stayed secure no matter Maclean what had done.[94] Yet it is possible that Maclean compromised Rockex. He was First Secretary at the Washington embassy and acting Head of Chancery from May to November 1946.[95] According to an internal NSA history as part of his duties he 'was in charge of the coderoom in Washington.'[96] This was particularly significant for the Foreign Office had installed its first Rockex in the Washington embassy in October 1944. Maclean was therefore perfectly placed to report to his controllers in Moscow on Britain's brand new Rockex cipher machine. He could inform them how it operated, take photographs and steal or copy key tapes, operating manuals and encrypted and plaintext telegrams. This would have given the Soviets an early start in devising ways to circumvent the Rockex's one-time cipher through technical surveillance and side channel attacks.

Hinchcliffe seems to have been a less serious case. He worked as an Assistant Administrative Officer at the British embassy in Khartoum and was blackmailed and bribed into acting as a Soviet agent between March 1970 and April 1971.[97] As well as giving the KGB Foreign Office documents he provided information about the embassy's cipher machines. Hinchcliffe told his contact the type of machine that the embassy operated and handed over a section of a cipher key that had been used to encrypt a telegram together with the plain text of the telegram and part of the encrypted text. However, Hinchcliffe was a reluctant spy and when he began a new posting in the Algiers embassy he confessed his past treachery to the British ambassador. At his subsequent trial in Britain the judge gave Hinchcliffe a reduced sentence, partly because he had only supplied his Soviet handler with 'material of a lower grade' and not the higher grade material that had also been available to him.[98] The cipher key, plaintext and encrypted text would have helped the Soviets understand how the embassy's cipher system functioned and identify it in other encrypted telegrams but it would not have given them a general solution to the cipher.[99]

Probably the most significant threat to Britain's machine ciphers came from Soviet technical surveillance and side channel attacks. By the 1950s the Soviets were using Tempest radiation to recreate the plain text from cipher machines and they could also exploit the sounds that the machines produced.[100] By monitoring the noises produced by the relays, switches, contacts and other components of a cipher machine, cryptanalysts could gather valuable information on the mechanism's workings.[101] Moreover, each key on the cipher machine key board might have a different acoustic signature when pressed and if a microphone was sensitive enough to pick up the differences between them, it would be possible to reconstruct a message typed into the cipher machine. The Soviets grouped these acoustic emissions and Tempest radiation as one information source and gave it the acronym PEMNI (Collateral Electromagnetic Emanation and Acoustic Emission).[102] The KGB was adept at using PEMNI to by-pass

sophisticated machine ciphers. When a new American embassy was constructed in Moscow in 1953 the Soviets secretly embedded 52 microphones in it and set a large metal grill in the ceiling of a room near the State Department communications centre with co-axial cables running off, possibly to detect Tempest radiation.[103] By analysing the PEMNI emissions a KGB team in 1959 could partially read the encrypted traffic of the embassy.[104] The KGB may have been reading the American communications earlier as embassy telegrams were listed among documents distributed to the Soviet Presidium in 1956.[105]

This raises the question of whether the KGB also mounted a PEMNI attack on the Rockex machines which had been in Britain's Moscow embassy since summer 1945. As yet, there is no evidence that the Soviets targeted the machines' Tempest radiation but they were able to plant bugs in the embassy. A security sweep in October 1959 uncovered three microphones in the building including one hidden in what had formerly been the cipher room.[106] The Soviets were thought to have installed the bugging system sometime between 1941 and 1943 when the diplomatic staff were temporarily evacuated from Moscow. The British authorities feared that the cipher room microphone may have enabled the Soviets to read the embassy's telegrams and they set up a working party to investigate.[107] In August 1960 the prime minister was advised that:

> …the Working Party concludes that (except during periods between 1945 and mid-1947 and November 1953 and January 1954 when the cypher room was elsewhere) information classified up to and including Top Secret was intermittently compromised from October 1943 until early in 1954, and to a lesser extent from then until late 1958. From that date until the discovery of the microphones in October 1959 the damage to classified information arose only from possible lapses of speech security due to human error and is likely to have been slight.[108]

The implication here is that the embassy's Rockex cipher machines were compromised by the bugging. Until KGB archives are opened, there is no way to confirm whether the Soviets could reconstruct the plain text of embassy telegrams from sounds captured by the microphone but considering the KGB's success against the American embassy, it does seem

possible.[109] It is notable that the Canadian embassy in Moscow, which operated either Rockex or Typex, also suffered a cipher breach in the early 1960s.[110] An agent in the embassy passed on cipher information to the KGB and planted bugs in the communications room which enabled the Soviets to intercept and decrypt every message passing between Moscow and Ottawa.

The discovery of the microphones in the British embassy drove the Foreign Office to take further action to protect its cipher machines from technical surveillance and side channel attacks. It built a special safe room in the Moscow embassy to house the cipher machines there and during the 1960s it constructed a further 24 cipher safe rooms in embassies where there was a high risk of technical surveillance.[111] As well as being sound proofed, these rooms were shielded to prevent the leakage of any Tempest radiation.[112] There was palpable nervousness in the Foreign Office about hostile technical surveillance of Rockex in posts without safe rooms. In 1968 the Foreign Office Security Department wanted to replace Rockex in Ankara, Bahrain and Rawalpindi 'as soon as possible, because of the technical insecurity associated with that system.'[113] The following year the Foreign Office instructed the British high commission in Wellington to revert back to using 'book cyphers' (most likely one-time pads) after an inspection found that the commission's Rockex cipher machines were emitting Tempest radiation well beyond the walls and ceiling of the cipher room.[114] For the Foreign Office the general replacement of Rockex by Alvis could not come soon enough.

The early Cold War was a period of transition for British communications security and cryptography. The Foreign Office and CRO moved away from time consuming manual ciphers and switched to mechanised encryption across their networks of embassies and high commissions. Enciphering and deciphering messages became quicker as a result and this helped speed up communications between London and its diplomatic missions. Cipher machine technology also rapidly advanced from rotor machines like Typex to the Rockex and

Noreen one-time tape machines and finally to Alvis, a tapeless, rotorless, transistor based device. These were technologically advanced, sophisticated cipher machines, equal to some of the best in the world and their development meant that in the early Cold War the Foreign Office's diplomatic communications were protected by far stronger cryptographic systems than in the 1930s. Indeed, the British were confident that some of their machine ciphers were unsolvable by pure cryptanalysis.

This did not necessarily mean though that British cipher machines provided complete security and secrecy for diplomatic communications. The danger came from physical compromise of cipher systems, technical surveillance and side channel attacks and in these areas Britain did have some failures in the early Cold War. It lost a Rockex in Beijing in 1967 and the Soviet agents Maclean and Hinchcliffe had free access to cipher machines and cryptographic material. Rockex had an extremely strong cipher but at the same time it was highly vulnerable to technical surveillance of its Tempest radiation and acoustic emissions. By bugging Britain's Moscow embassy the Soviets seem to have been able to read the diplomatic traffic enciphered and deciphered by the Rockex machines there in the late 1940s and early 1950s.

Yet complete communications security is perhaps impossible to achieve, particularly over a 25-year period, and Britain did not fare comparatively worse than some of its UKUSA partners. The United States and Canada also suffered from Soviet espionage and had their diplomatic ciphers broken through the bugging of embassies in Moscow. The United States had cryptographic material snatched from its embassy in Taipei in 1957 when it was stormed by protestors.[115] Rockex's Tempest radiation was a weak point but the British did discover this vulnerability early on and took a series of counter measures. They modified Rockex to reduce the emissions, limited which embassies it was deployed in, employed Noreen as a partial replacement and built safe rooms to shield it from Tempest and acoustic attacks. Other

countries were much slower in discovering Tempest radiation and their cipher machines remained unprotected, which was something that GCHQ itself exploited. Peter Wright recounted in his memoirs how GCHQ, MI5 and MI6 used Tempest radiation to break the diplomatic ciphers of France and other states in the 1960s.[116] So while Britain's cipher security record in the early Cold War was not perfect, it did secure its diplomatic secrets better than many other states.

## Notes

[1] Aldrich, *GCHQ;* Aid, *The Secret Sentry*; Budiansky, *Code Warriors.* See also Aid and Wiebes, *Secrets of Signals Intelligence*.
[2] Aldrich, *GCHQ,* 55-57,191-192, 209-212, 241-242; Aldrich, *Whitehall wiring.*
[3] Ferris, *The British Enigma*; Smith, *Bletchley Park.*
[4] Ferris, *The British Enigma,* 138.
[5] The websites http://www.cryptomuseum.com/ and http://www.jproc.ca/crypto/menu.html also have valuable technical information about the cipher machines.
[6] The National Archives (TNA), FO 850/134, File note, 6 February 1944; Minute Travis to Sargent, 12 June 1944; CAB 116/30, War Cabinet Paper, S(42) 27 'Cypher Security', 29 September 1942; Ferris, *The British Enigma,* 157.
[7] Aldrich, 'Whitehall wiring', 181.
[8] Aldrich, *GCHQ,* 55-57.
[9] TNA, DEFE 32/18, Minute Burroughs to Ryland, Annex A, 3 June 1969.
[10] Ferris*, The British Enigma*, 177-178; TNA, DEFE 32/18, Minute Burroughs to Ryland, Annex A, 3 June 1969; TNA, T 220/1406, Minute by Rampton, CPB (62) 1, 'Services Communication Development Unit', 20 January 1953; TNA, DEFE 5/58, Memorandum COS (55) 113, 11 May 1955.
[11] TNA, DEFE 32/18, Minute Burroughs to Ryland, Annex A, 3 June 1969.
[12] Aldrich, *GCHQ,* 103, 191-192; Aldrich, *Whitehall wiring*, 182-183; TNA, DEFE 32/18, Minute Burroughs to Ryland, Annex A, 3 June 1969; NSA, William F. Friedman Collection of Official Papers (https://www.nsa.gov/public_info/declass/friedman_documents/index.shtml), Memorandum USCIB: 12./7, Taylor to United States Communications Intelligence Board, enclosure, 18 October 1954; http://discovery.nationalarchives.gov.uk/details/r/C9288 (Accessed 20 January 2017). It was renamed the London Communications –Electronics Security Agency in 1958. See http://www.nationalarchives.gov.uk/documents/information-management/osp28.pdf (Accessed 13 July 2015).
[13] TNA, DEFE 32/18, Minute Burroughs to Ryland, Annex A, 3 June 1969.
[14] Ibid.; NSA, William F. Friedman Collection of Official Papers, Memorandum USCIB: 14.3/12, to U.S. Communications Intelligence board, enclosure, 24 June 1955.
[15] Aldrich, *Whitehall wiring*, 183.
[16] TNA, DEFE 32/18, Minute Burroughs to Ryland, Annex A, 3 June 1969.
[17] Ferris, *The British Enigma*, 171-174; Smith, *Bletchley Park,* 187, 189-190; http://www.jproc.ca/crypto/rockex.html (Accessed 24 April 2018).
[18] Ferris, *The British Enigma*, 172; TNA, CO 1038/3, Memorandum titled 'Mr Robinson, Mrs. Sander and I visited the F.O. Cypher Training School on 18th July', not dated.
[19] Ferris, *The British Enigma,* 174-175.
[20] TNA, FO 850/134, Tel 5716 Washington to FO**,** 21 October 1944; FO 850/192, Letter 465 Clark-Kerr to Eden, 9 July 1945; FO 850/172 Telegram 3747 Clark-Kerr to Foreign Office, 24 August 1945.
[21] TNA, HW 9/27, CPB (48) 1, 'Report by Secretary for the year ended 31st July 1948, 19 February 1949.
[22] TNA, FO 371/96594, Noted by Orchard, 17 November 1950.
[23] TNA, HW 9/27, CPB (48) 1, 'Report by Secretary for the year ended 31st July 1948, 19 February 1949.
[24] Anonymous, 'TEMPEST: A Signal Problem', *Cryptologic Spectrum*, 3/3 (1972), NSA, http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf (Accessed 10 July 2015).
[25] Aldrich, *GCHQ*, 215-218; Aldrich, *Whitehall wiring*, 182.
[26] NSA, Friedman Collection, Memorandum LCS (53)/N/R 'U.S. Communications Security Equipments and U.K. Cryptographic Equipments', not dated. See also http://www.cryptomuseum.com/crypto/uk/rockex/index.htm (Accessed 19 May 2018).
[27] Ferris, *The British Enigma,* 174.
[28] TNA, HW 9/27, CPB(49) 14 'Report by the Secretary for the year ended 31st July 1949', 1 March 1950.
[29] TNA, T 220/1406, Letter Burton-Miller to Drake, covering CPB (52) 1, Services Communications Development Unit, 17 December 1952; Minute Rampton, 20 January 1953.
[30] NSA, Friedman Collection, Memorandum LCS (53)/N/R 'U.S. Communications Security Equipments and U.K. Cryptographic Equipments', not dated.

[31] TNA, WO 32/20548, Telegram Sigs 422, FARELF to War Office, 11 March 1957; Note by G. Mitchell, Signals, 21 February 1957.
[32] Ferris, *The British Enigma*, 152-153.
[33] Ibid., 163-164.
[34] TNA, HW 9/27, CPB (48) 1, 'Report by the Secretary for the year ended 31st July 1948', 19 February 1949.
[35] Ibid; NSA, Friedman Collection, Minute Austin to Friedman, 14 September 1953, covering memorandum on 'U.K. Cryptographic Equipments', not dated.
[36] TNA, HW 9/4, 'Notes on the 14th X/L Production Meeting', 14 August 1950; HW 9/27, CPB (48) 1, 'Report by the Secretary for the year ended 31st July 1948', 19 February 1949.
[37] NSA, Friedman Collection, Memorandum LCS (53)/N/R 'U.S. Communications Security Equipments and U.K. Cryptographic Equipments', not dated.
[38] TNA, CAB 21/4604, Minute Bennett to Thuiler, 28 March 1960.
[39] Ibid.
[40] TNA, CO 1038/3, Minute Costley-White to Gidden, 7 June 1963.
[41] TNA, CAB 21/4604, Minute Vincent to Stannard, 28 September 1962; CO 1038/3, Minutes of the Second Meeting of the Working Party on Integration of Foreign Office and CRO systems, 12 July 1963.
[42] TNA, FO 850/325, Letter TB38/94/1 Pope to Routledge, 9 October 1964.
[43] TNA, FO 850/325, Letter Milner to Vincent, 12 November 1964; CO 1038/3, Memorandum titled 'Mr Robinson, Mrs. Sander and I visited the F.O. Cypher Training School on 18th July', not dated; FCO 19/168, Memorandum by Routledge, 14 October 1971.
[44] National Archives of Australia (NAA), A1838, TS1218/11/1 Part 1, Minute Moodie to The Secretary, 16 August 1963; TNA, FCO 19/86, Minute Routledge to Snelling, 17 June 1971; Dunningham, *From Telegrams to eGrams,* 18.
[45] TNA, FCO 19/2, Letter Crowe to Head of Post, attachment valedictory report '4 ½ Years in the Communications Department', 25 January 1967.
[46] TNA, FCO 19/86, Minute Routledge to Snelling, 17 June 1971.
[47] TNA, CO 1038/3, Minute Darby to Clemens, 22 January 1964,
[48] TNA, FCO 19/159, Communication Systems Working Party Forward Planning Sub-Committee, Note of a meeting held on 10 November 1970, not dated.
[49] TNA, FCO 19/168, Memorandum by Routledge, 14 October 1971.
[50] TNA, FCO 19/86, Minute Routledge to Snelling, 17 June 1969; Letter Gardiner to Snelling, 16 July 1969; FCO 19/2, Letter Crowe to Head of Post, attachment valedictory report '4 ½ Years in the Communications Department.' 25 January 1967; FCO 19/159, Minutes of Communications systems working party, 12th Meeting on 17 February 1970, not dated.
[51] TNA, DEFE 59/16, Memorandum DSS 23/64 (Final), 26 May 1965.
[52] TNA, DEFE 5/90, Memorandum COS(59) 82, Annex, 14 April 1959.
[53] TNA, T 225/2074, Letter Stannard to Orchard, 26 July 1962; Minutes of Meeting at Foreign Office on 'Provision of on-line cryptographic equipment for NATO', 24 July 1962.
[54] TNA, FCO 19/159, Minutes of Communications Systems Working Party, 12th Meeting on 17 February 1970, not dated.
[55] TNA, FCO 19/159, Communication Systems Working Party, Forward Planning Subcommittee, Minutes 2nd meeting held on 17 December 1970, not dated.; Communication Systems Working Party, Forward Planning Sub Committee, Note of meeting held on 10 November 1970, not dated.
[56] TNA, FCO 19/159, Communication Systems Working Party, Forward Planning Sub Committee, Note of meeting held on 10 November 1970, not dated.
[57] Aid, *Secret Sentry,* 11-13; Aldrich, *GCHQ,* 90; TNA, DEFE 59/19, Memorandum DSS 34/66 (Final), Annex A, 21 November 1966.
[58] NAA, A1838, 1218/13/7, Letter Under Secretary of State, Air Ministry to Australian High Commission, London, 21 April 1949; Minute JPW to the Assistant Secretary, 25 August 1953; A1838, TS1218/11/1 Part 1, Minute External Communications Branch to Assistant Secretary (Division 3), 11 August 1961.
[59] NAA, A1838, TS1218/11/1 Part 1, Minute Walshe to Bennett, 29 January 1957; Minute External Communications Branch to Assistant Secretary (Division 3), 11 August 1961; Minute Moodie to the Secretary, 16 August 1963; TNA, FCO 19/29, Minute AN05K/7966 CESD to Ministry of Defence, 21 June 1968; Aldrich, *GCHQ*, 586.

[60] TNA, HW 9/27, CPB (48) 1, 'Report by Secretary for the year ended 31st July 1948, 19 February 1949; CAB 21/4604, Minute Costley-White to Gardiner, Attachment 'Cypher Machines Held by the C.R.O. and Commonwealth Governments', 21 June 1960; Aldrich, *GCHQ,* 586.
[61] TNA, CAB 21/4604, Minute Costley-White to Gardiner, Attachment 'Cypher Machines Held by the C.R.O. and Commonwealth Governments', 21 June 1960. There is a reference to New Zealand as well as Australia and Canada potentially needing Rockex spare parts in TNA, FCO 19/168, Letter Holden to Bayley, 1 December 1971.
[62] TNA, CAB 21/4604, Minute Costley-White to Gardiner, Attachment 'Cypher Machines Held by the C.R.O. and Commonwealth Governments', 21 June 1960.
[63] TNA, CAB 21/4604, 'Note of an informal meeting held in General Thuiller's office', 18 August 1961; Draft memorandum 'Foreign Service Technical Maintenance. Installation and Maintenance of Telephone Equipment at Commonwealth Overseas posts', not dated.
[64] TNA, CAB 21/4604, Minute Costley-White to Gardiner, Attachment 'Cypher Machines Held by the C.R.O. and Commonwealth Governments', 21 June 1960; Note of an informal meeting held in General Thuiller's office', 18 August 1961.
[65] NAA, A1838/1218/13/7, Minute Under-Secretary of State, Air Ministry to Australian High Commission, London, 21 April 1949; NAA, A705/201/33/441, Letter Director of Signals, Air Ministry to Director of Signals to Commander in Chief F.E.A.F., 18 June 1949.
[66] TNA, FCO 19/23, Minutes Eaden to Bates, 5 January 1968; Minute Bates to Snelling, 19 March 1968.
[67] Haslam, *Near and Distant Neighbours,* 173.
[68] Andrew, *KGB,* 459.
[69] TNA, CAB 21/4604, Minute Bennett to Thuiler, 28 March 1960.
[70] Ratcliff, *Delusions,* 120.
[71] TNA, CAB 21/4604, Minute Bennett to Thuiler, 28 March 1960.
[72] NAA, A1838, TS1218/11/1, Part 1, UKCSC Minutes, 256th Meeting, Extract No. 23/1951, 9 March 1951.
[73] TNA, CAB 21/4003, Memorandum COMSECA (56) 5, 'Personal Security Rules for Cypher Staffs', by LCSA, 30 July 1956.
[74] Sebag-Montefiore, *Enigma,* 1, 113-115.
[75] TNA, WORK 10/479, Letter 137, Wright to Foreign Office, 21 August 1958; Aldrich, *GCHQ,* 193; TNA, FO 366/3357, Telegram 2102, Trevelyan to Foreign Office, 10 October 1964.
[76] 'Believe it or not' by J. G. L., Leger Roy, The Old Foreign Affairs Retired Technicians Canada Website, http://ofarts.ca/Index_files/articles/believeitornot/believeitornot.htm (Accessed 16 February 2018)
[77] The Churchill Archives Centre, Sir Andrew Gilchrist Papers, Box 13/A, File 'September 23 1963', not dated.
[78] John F. Kennedy Presidential Library, National Security Files, Box 114A, File Indonesia General 9/63, Telegram 676, Jakarta to State Department, 23 September 1963.
[79] *The Canberra Times,* 'British Remove Embassy Secrets', p. 1, 25 September 1963; The Churchill Archives Centre, Sir Andrew Gilchrist Papers, Box 13/A, File 'Djakarta – September 1963', not dated.
[80] Aldrich, *GCHQ,* 193-194.
[81] Ibid. 194.
[82] Churchill Archives Centre, Diplomatic Oral History Programme, Interview with Sir John Weston, https://www.chu.cam.ac.uk/media/uploads/files/Weston_l8PHksY.pdf (Accessed 19 March 2018); Shah, *Secret Towns,* 136.
[83] Churchill Archives, Interview with Sir John Weston.
[84] See also Shah, *Secret Towns,* 135-136.
[85] Churchill Archives, Interview with Sir John Weston; Shah, *Secret Towns,* 135-136.
[86] TNA, CO 1038/3, Memorandum, 'Emergency destruction of Rockex machines and ancillary equipment', not dated.
[87] Andrew and Gordievsky, *KGB,* 195-197; Andrew, *Defence of the Realm,* 263-264.
[88] Andrew, *Defence of the Realm,* 264.
[89] Aldrich, *Hidden Hand,* 422-424.
[90] Aldrich, *GCHQ,* 83-84.
[91] Benson, *The Venona Story,* 15, 34-35. https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/assets/files/venona_story.pdf (Accessed March 10 2018).
[92] Wright, *Spycatcher,* 292.
[93] Cecil, *A Divided Life,* 135.
[94] Ibid.

[95] Ibid., 117, 126.
[96] Johnson, *American Cryptology,* 165.
[97] *The Times,* 'Trusted Foreign Office man who became spy through fear jailed for 10 years', p. 3, 18 April 1972; *The Guardian, '*10 years for embassy cipher man in Soviet spy trap', p. 7, 18 April 1972.
[98] *The Guardian,* '10 years for embassy cipher man'.
[99] Ibid.
[100] Johnson, *American Cryptology*, 221.
[101] Easter, 'Soviet Bloc and Western Bugging', 32.
[102] Haslam, *Near and Distant Neighbours,* 241.
[103] Easter, 'Soviet Bloc and Western Bugging', 34-36.
[104] Haslam, *Near and Distant Neighbours,* 241.
[105] Fursenko and Naftali, *Khrushchev's Cold War,* 93, 560.
[106] Easter, 'Soviet Bloc and Western Bugging', 34.
[107] TNA, PREM 11/3104, Minute Acland to de Zulueta, 15 August 1960.
[108] Easter, 'Soviet Bloc and Western Bugging', 43-44.
[109] It is conceivable that Maclean supplied information which helped the Soviets attack the Moscow Rockex machines but no evidence for this has come to light.
[110] Sawatsky, *Men in the Shadows,* 138-141; Ford, *Our Man in Moscow,* 151. It is not known which type of cipher machine was in the embassy but at that time the Canadian Department of External Affairs operated Rockex and Typex. TNA CAB 21/4604, Memorandum 'Cypher Machines Held by the C.R.O. and Commonwealth Governments', not dated; 'Communications Rooms at Canadian Embassies' by Thurlow Arbuckle, http://www.jproc.ca/crypto/canadian_embassy.html (Accessed 13 June 2018).
[111] Easter, 'Soviet Bloc and Western Bugging', 40-41; TNA, FCO 19/86, Minute by Askew, 25 June 1969.
[112] Aldrich, *GCHQ,* 196-197.
[113] TNA, FCO 19/18, Cypher Security Working Party, Note of Eighth Meeting held in DSAO on 1 October 1968, 1 October 1968.
[114] TNA, FCO 19/90, Letter Griffiths to Tonkin, 13 January 1969; Report 'British High Commission Wellington' by Murray and Williams, not dated.
[115] Aldrich, *GCHQ,* 195.
[116] Wright, *Spycatcher,* 109-114.

## Bibliography


Aid, Matthew and Wiebes, Cees, eds,, *Secrets of Signals Intelligence during the Cold War and Beyond*, London: Frank Cass, 2001.

Aid, Matthew, *The Secret Sentry: The Untold History of the National Security Agency,* New York: Bloomsbury Press, 2009.

Aldrich, Richard, *The Hidden Hand: Britain, American and Cold War Secret Intelligence,* New York: Overlook Press, 2002.

Aldrich, Richard, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency,* London: Harper Press, 2010.

Aldrich, Richard, 'Whitehall wiring: The Communications Electronics Security Group and the struggle for secure speech', *Public Policy and Administration,* 28, no. 2 (2012): 178-195.

Andrew, Christopher and Gordievsky, *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev,* London: Sceptre, 1991.

Andrew, Christopher, *The Defence of the Realm: The Authorised History of MI5,* London: Pearson, 2010.

Benson, Robert, *The Venona Story,* Fort Meade, Centre for Cryptologic History NSA, not dated.

Budiansky, Stephen, *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union,* New York: Alfred A, Kopf, 2016.

Cecil, Robert, *A Divided Life: A Biography of Donald Maclean,* London: Coronet Books, 1990.

Dunningham, Bill, *From Telegrams to eGrams: A Potted History of FCO Communications,* London: Foreign and Commonwealth Office, 2004.
Easter, David, 'Soviet Bloc and Western Bugging of Opponents' Diplomatic Premises during the Early Cold War, *Intelligence and National Security,* 31, no. 1, (2016): 28-48.
Ferris, John Robert, 'The British "Enigma": Britain, Signals Security and Cipher Machines, 1906-1953', in John Ferris, *Intelligence and Strategy: Selected Essays*, London: Routledge, 2005.
Ford, Robert, *Our Man in Moscow: A Diplomat's Reflections on the Soviet Union*, Toronto: University of Toronto Press, 1989.
Haslam, Jonathan, *Near and Distant Neighbours: A New History of Soviet Intelligence,* Oxford: Oxford University Press, 2015.
Johnson, Thomas. *American Cryptology during the Cold War, 1945-1989, Book I: The Struggle for Centralization, 1945-1960*, Fort Meade: Centre for Cryptologic History NSA, 1995.
Fursenko, Aleksandr and Naftali, Timothy, *Khrushchev's Cold War: The Inside Story of an American Adversary,* New York: W. W. Norton, 2006.
Ratcliff, R. A., *Delusions of Intelligence: Enigma, Ultra and the End of Secure Ciphers,* Cambridge: Cambridge University Press, 2006.
Sawatsky, John, *Men in the Shadows: the RCMP Security Service,* Toronto: Doubleday Canada Limited, 1980.
Sebag-Monefiore, Hugh, *Enigma: The Battle for the Code,* London: Phoenix, 2001.
Shah, Nikita, "'Secret Towns': British Intelligence in Asia during the Cold War", PhD diss., University of Warwick, 2016.
Smith, Christopher, 'Bletchley Park and the Development of the Rockex Cipher System: Building a Technocratic Culture, 1941-1945', *War in History,* 24, no. 2, (2017): 176-194.
Wright, Peter, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer,* Toronto: Stoddart Publishing Company, 1987.